산업제어시스템 정보보안 관리체계 프로그램 개발

천세인**, 주소영*, 김민주**, 백지연*, 신자은*
*성신여자대학교 융합보안(공)학과
**성신여자대학교 IT 학부
e-mail : imsichun@naver.com, zoocinei@naver.com, kimmin47@naver.com, hesedbaek@gmail.com, jaeuns1@gmail.com,

Development of an Industrial Control System Information Security Management System Program

Se-In Chun**, Soyoung Joo*, Min-Ju Kim**, Ji-Yeon Baek*, Jaeun Shin*
*Dept. of Convergence Security (Engineering), Sung-Shin Women's University
**Dept. of IT, Sung-Shin Women's University

요 약

주요기반시설 산업제어시스템의 운영환경 변화에 따라 보안 위협의 양상이 다양해지고 있다. 따라서 이를 반영한 보안 관리체계가 새로이 요구된다. 이에 본 논문은 미국 <*Reg Guide 5.71*>과 <*NEI 13-10*>을 참조한 산업제어시스템의 정보보안 관리체계 프로그램을 제안한다. 프로그램의 기능은 다음과 같다. 첫째, 산업제어시스템 자산 관리 기능, 둘째, 보안상태 평가 기능, 셋째, 보안조치 관리 기능이다. 해당 프로그램을 통해 국내 산업제어시스템의 보안 수준 향상을 기대한다.

1. 서론

산업제어시스템(ICS, Industrial Control System)은 사회 주요기반시설의 설비를 효과적으로 제어하기 위해 사용되는 컴퓨터 기반의 시스템을 말한다.[1]

기존 대부분의 산업제어시스템은 폐쇄 네트워크로 운영되었으나 최근에는 정보통신 서비스와 연결되어 운영되고 있다.[2] 이에 따라 상용 IT 환경에서 존재하던 보안 위협인 비인가 접속 공격, DDOS 공격, APT 공격 등이 산업제어시스템 환경에도 발생하고 있다.[3][4]

그럼에도 주요기반시설 산업제어시스템의 보안조치는 기존 환경에서 수립된 채로 유지되고 있어 새로운 위협에 대응하지 못하고 있다.[5] 따라서 급격히 변화하는 제어시스템 및 보안 분야의 기술적, 제도적 환경에 능동적으로 대응할 수 있는 보안 관리체계의 개발이 필요하다.[6]

우리나라보다 앞서 이러한 문제를 직면한 미국의 경우 산업제어시스템의 규제 및 표준을 제정하여 관리하고 있다. 본 논문은 미국 ICS 규제 가이드 <*Reg Guide 5.71*>과 미국 원자력협회의 <*NEI 13-10*>을 참조하여 국내 상황에 적합한 산업제어시스템 정보보안 관리체계 프로그램을 제안하고자 한다.

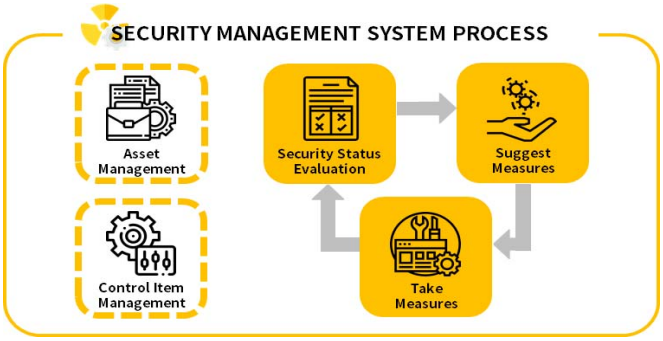
본 프로그램의 주요 특징은 크게 세가지로 나눌 수 있다. 첫째, 산업제어시스템의 자산관리 기능을 제공한다. 국가 핵심기반 산업시설 내 자산을 자산 속성과 함께 등록하여 속성별 세부 관리가 가능하게 한다.

둘째, 보안상태 평가 기능을 제공한다. <*Reg Guide 5.71*> 중 국내 산업제어시스템 보안 상황에 적합한 일부를 발췌하여 프로그램의 통제항목으로 등록한다. 이를 바탕으로 산업제어시스템의 보안상태를 평가하고 그 결과를 관리함으로써 산업제어시스템의 현재 보안 수준을 체계적으로 가늠할 수 있다.

셋째, 자산 별 보안조치 관리 기능을 제공한다. 프로그램은 <*NEI 13-10*>을 기반으로 각 자산의 속성에 따라 취해야할 보안조치를 알고리즘을 통해 분석하여 제시한다. 이때 조치 가능여부에 따라 대안조치를 추가 제안함으로써 효율적 보안조치가 가능하다.

본 논문은 다음과 같이 구성된다. 2 장에서는 산업제어시스템 정보보안 관리체계 프로세스를 제시하고 3 장에서는 이를 기반으로 한 프로그램의 알고리즘 및 기능을 설명한다. 4 장에서는 프로그램의 구현 결과를 설명하고 5 장에서는 기대효과와 향후 연구방향을 제시하며 결론을 짓는다.

2. ICS 정보보안 관리체계 프로세스



(그림 1)ICS 정보보안 관리체계 프로세스

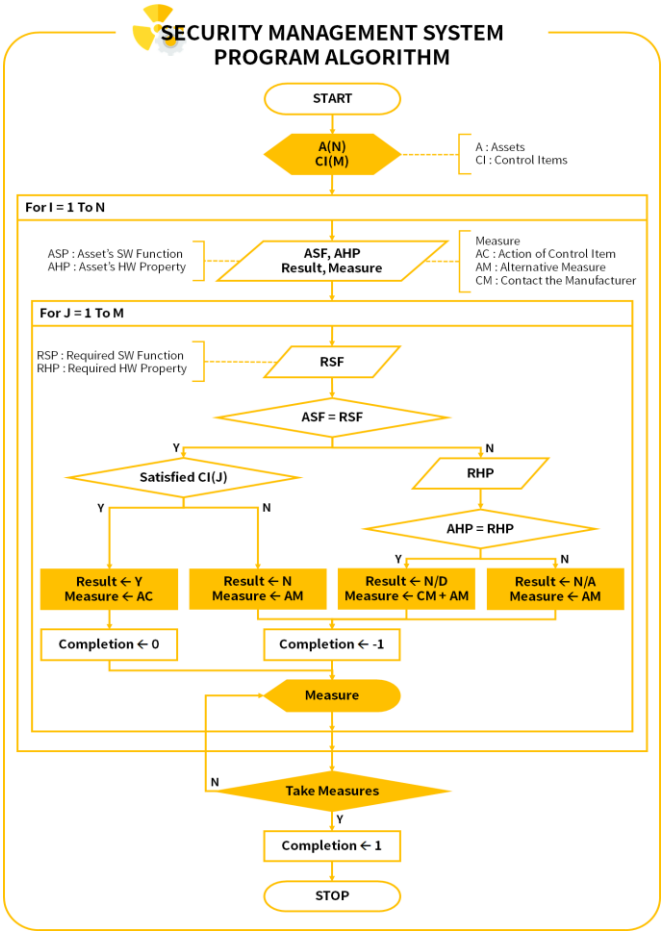
그림 1 은 본 논문에서 제시하는 산업제어시스템의 정보보안 관리체계 프로세스를 나타낸다.

프로세스는 크게 평가 전단계와 평가 및 조치단계 두 가지로 나뉜다. 평가 전단계에서는 자산 관리(Asset Management)와 통제항목 관리(Control Item Management)를 수행한다. 산업제어시스템의 자산과 보안 통제항목을 등록, 관리함으로써 보안상태 평가를 위한 준비를 한다.

평가 및 조치단계에서는 평가 전단계에서 준비된 자산과 통제항목 정보를 기반으로 보안상태 평가(Security Status Evaluation)를 실시한다. 평가 결과, 보완이 필요한 경우 적절한 보안조치를 제안(Suggest Measures)하여 조치를 취하도록(Take Measures) 한다. 한 사이클이 끝나면 재평가를 실시하여 산업제어시스템의 정보보안 관리를 지속적으로 유지, 보수할 수 있도록 한다.

3. ICS 정보보안 관리체계 프로그램

3.1. 프로그램 알고리즘



(그림 2)ICS 정보보안 관리체계 프로그램 알고리즘

그림 2 는 1 장에서 제시한 프로세스를 기반으로 하는 산업제어시스템 정보보안 관리체계 프로그램의 알고리즘을 도식화한 것이다.

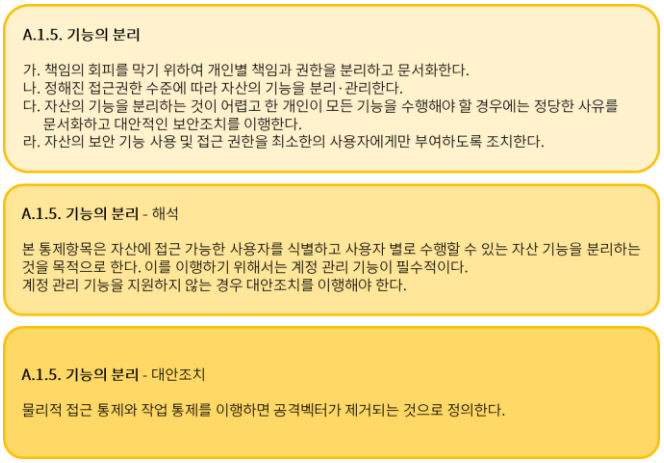
프로그램의 초기 설정으로 1 단계, 산업제어시스템의 자산(A(N))과 정보보안 관리를 위한 통제항목(CI(M))를 등록한다. 2 단계, 등록한 N 개의 자산을 보안상태 평가 대상으로 한다. 3 단계, 각 자산의 보안상태 평가를 반복문으로 수행한다.

보안상태 평가 반복문은 등록된 통제항목 수(M)만큼 수행된다. 먼저 선택한 자산의 SW 기능(ASF, Asset's SW Function)과 평가할 통제항목(CI(J))에서 요구되는 SW 기능(RSP, Required SW Function)을 비교한다. 비교 결과가 동일(필요한 SW 기능을 모두 지원)할 경우, 해당 자산이 통제항목 CI(J)를 만족시키고 있는지 판단한다. 통제항목을 만족시킬 경우에는 평가 결과가 Y 가 되고 통제항목을 만족시키기 위한 조치(AC, Action of Control Item)를 제시한다. 통제항목을 만족시키지 않는(필요한 SW 기능을 지원하지 않는) 경우에는 결과가 N 이 되며 통제항목 조치를 대체할 수 있는 적절한 대안조치(AM, Alternative Measure)를 제시한다.

SW 기능 비교 결과가 동일하지 않을 경우, 자산의 HW 속성(AHP, Asset's HW Property)과 통제항목에서 요구되는 HW 속성(RHP, Required HW Property)을 비교한다. HW 속성 비교 결과가 동일할(SW 기능을 구현할 수 있는 HW 속성을 보유하고 있는) 경우에는 평가 결과가 N/D 가 된다. 이 경우 제조사에 문의하여 필요한 SW 기능 구현 가능 여부를 확인(CM, Contact the Manufacturer)하도록 제안한다. 이때 문의 답변이 오기 전까지, 혹은 문의 결과 구현이 불가능할 경우 수행할 대안조치(AM)를 함께 제시한다. HW 속성 비교 결과가 동일하지 않을(SW 기능을 구현할 수 있는 HW 속성을 보유하고 있지 않은) 경우에는 평가 결과가 N/A 가 되며 앞선 N 과 N/D 와 동일하게 대안조치(AM)를 제시한다.

4 단계, 모든 통제항목에 대해 평가가 완료되면 제안된 조치들을 수행(Take Measures)하도록 요구된다. 본 프로그램은 이러한 알고리즘을 통해 산업제어시스템 내 모든 자산의 보안상태 평가를 정기적으로 시행함으로써 지속적 정보보안 관리를 할 수 있도록 한다.

3.2. 보안상태 평가 과정



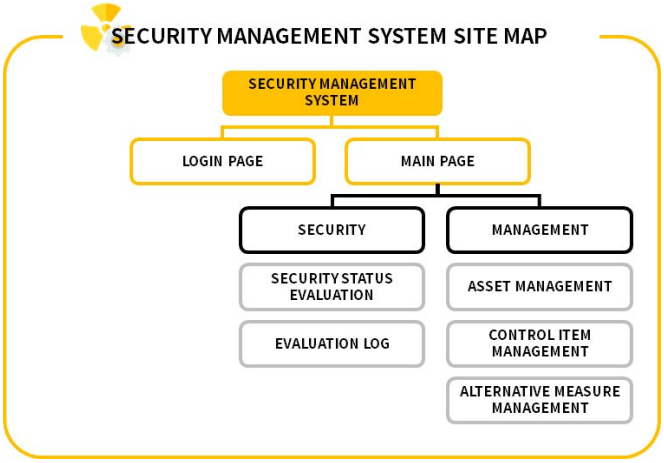
(그림 3)보안상태 평가 과정 예시

그림 3 은 3.1 장에서 설명한 보안상태 평가의 이해를 돕기 위해 예시를 든 것이다.

먼저 <*Reg Guide 5.71*>에서 발췌하여 등록한 통제항목을 해석하여 관련 보안통제 시 필요한 요건들을 판단한다. 예시인 통제항목 A.1.5 의 경우, 관련 내용(<*Reg Guide 5.71*> 中 B.1.5)을 해석하면 계정 및 권한 관리 기능이 요구된다는 것을 알 수 있다. 해당 SW 기능을 지원하는 자산은 통제항목 만족 여부에 따라 결과가 Y 또는 N, 지원하지 않은 자산은 결과가 N/A, N/D 중 하나가 된다.

통제항목 해석 결과 대안조치가 필요한 경우, <*NEI 13-10*>을 기반으로 적절한 대안조치를 제안한다. 예시인 A.1.5 는 관련 내용(<*NEI 13-10*> 中 C.4.3, C.5.5)에 따라 위와 같은 대안조치를 갖게 된다.

3.3. 프로그램 세부 기능



(그림 4)ICS 정보보안 관리체계 프로그램 화면구성도

그림 4 는 본 논문에서 제시하는 산업제어시스템 정보보안 관리체계 프로그램의 화면구성을 나타낸다.

프로그램 화면은 관리(Management) 탭, 보안(Security) 탭으로 이루어진 메인 페이지와 로그인 페이지로 구성된다.

<표 1> 관리 탭 세부내용_자산 관리

ATTRIBUTE NAME	DETAILED
자산명	-
자산속성	Security, Safety
자산유형	기록계, 전송기, PLC, DCS, PC, 서버류, 기타
운영체제	전용OS, 범용OS, 펌웨어, 기타
SW 기능	계정 관리, 암호 정책, 계정 잠금 정책, 감사 정책, 통신 암호화, 파일 공유, 원격 설정, 시간 동기화, CMOS/BIOS 설정
HW 속성	ROM, Flash Memory, HDD, 시리얼 통신, TCP/IP, 기타
활성상태	활성, 비활성

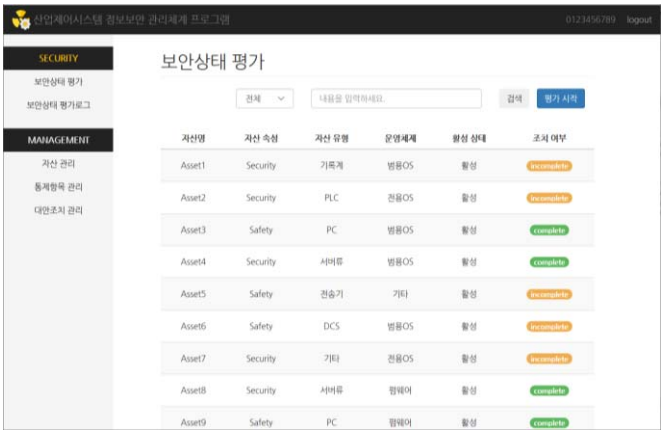
<표 2> 관리 탭 세부내용_통제항목 관리

MAJOR		MINOR
A.1	접근 통제	.1. 접근 통제 정책 및 절차, .2. 계정 관리, [···], .23. 공개 접근 가능 컨텐츠
A.2	감사와 책임	.1. 감사와 책임 정책 및 절차, .2. 감사 대상 이벤트, [···], .12. 감사 생성

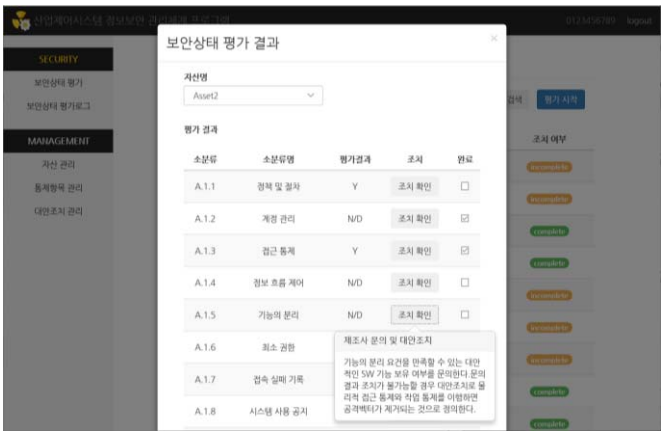
관리 탭에는 자산 관리(Assets Management) 메뉴, 통제항목 관리(Control Item Management) 메뉴, 대안조치 관리(Alternative Measure Management) 메뉴가 있다. 자산 관리 메뉴에서는 자산을 등록, 활성, 비활성 한다. 자산 등록 시 <표 1>의 속성값들을 선택하여 자산을 세부적으로 관리할 수 있도록 한다. 통제항목 관리 메뉴에서는 통제항목을 <표 2>와 같이 대분류와 소분류로 나누어 등록, 관리한다. 이때 각 통제항목에서 요구되는 자산의 SW 기능과 HW 속성을 함께 선택한다. 대안조치 메뉴에서는 각 통제항목에 대응하는 대안조치를 등록하여 관리한다. 관리 탭 내 모든 메뉴는 조건검색을 통해 목록을 조회할 수 있다.

보안 탭에는 보안상태 평가(Security Status Evaluation) 메뉴와 보안상태 평가 로그(Evaluation Log) 메뉴가 있다. 보안상태 평가 메뉴에서는 3.1 장에서 설명한 알고리즘에 따라 보안상태 평가를 실시한다. 평가가 완료되면 평가 결과와 필요한 조치가 제시된다. 평가 결과는 차후에도 확인할 수 있으며 조치를 취했을 경우 이를 체크하여 조치 여부를 관리할 수 있다. 보안상태 평가 로그 메뉴에서는 보안상태 평가 결과를 시간순으로 확인할 수 있어 추적관리가 가능하다. 각 로그를 선택하면 평과 결과와 함께 평가 세부 내용(평가자, 평가 시간 등)을 확인할 수 있다.

4. 프로그램 구현 결과



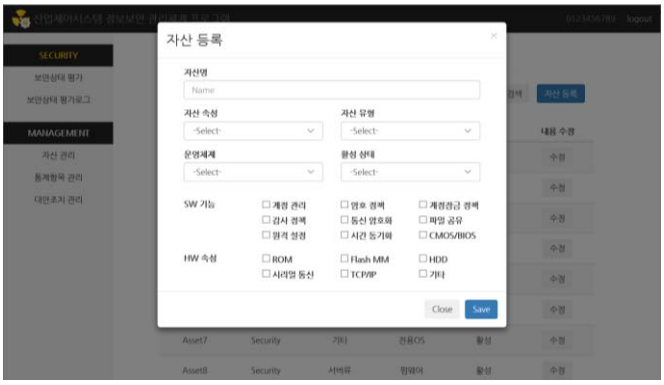
(그림 5)프로그램 구현 결과_보안상태 평가 메뉴



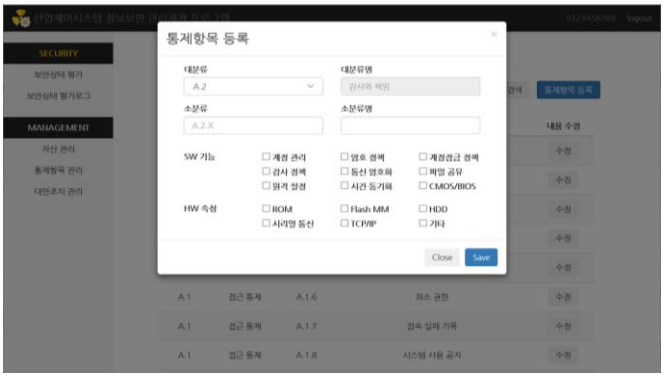
(그림 6)프로그램 구현 결과_보안상태 평가 결과

그림 5 와 그림 6 은 보안 탭의 보안상태 평가 메뉴

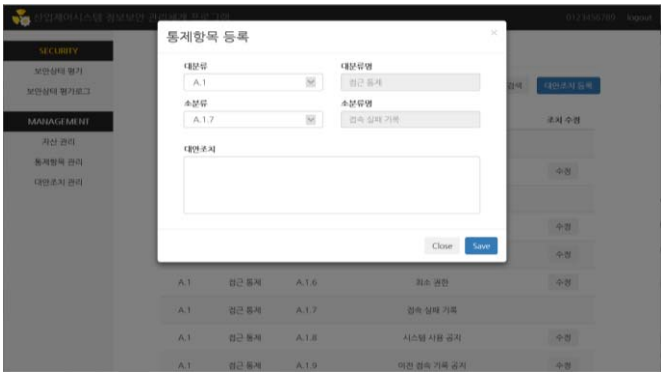
이다. 해당 페이지에서는 자산 관리 메뉴에서 등록한 전체 자산 목록이 나타난다. 평가 시작 버튼을 누르면 전체 자산에 대한 평가 결과 창이 나타난다. 평가 결과는 자산별로 확인 가능하며 각 통제항목에 해당하는 평가 결과와 조치 내용을 확인할 수 있다. 또한 조치 완료 시 체크를 통해 조치 여부를 저장할 수 있다. 조치 여부는 페이지의 자산 목록에서 complete 와 incomplete 로 구분되어 나타나므로 손쉽게 확인 후 수정이 가능하다.



(그림 7)프로그램 구현 결과_자산 등록



(그림 8)프로그램 구현 결과_통제항목 등록



(그림 9)프로그램 구현 결과_대안조치 등록

그림 7 은 관리 탭의 자산 관리 메뉴이다. 해당 페이지에서는 자산을 등록, 관리할 수 있다. 자산 등록 버튼을 누르면 속성값을 입력하여 신규 자산을 등록할 수 있다. 등록한 자산은 페이지에서 자산 목록으로 나타나며 수정 버튼을 통해 속성값을 수정할 수 있다. 모든 자산은 조건 검색을 통해 조회할 수 있다.

그림 8 은 관리 탭의 통제항목 관리 메뉴, 그림 9 는 관리 탭의 대안조치 관리 메뉴이다. 통제항목 페이지에서는 통제항목의 대분류를 선택하여 소분류 통제항목을 추가할 수 있다. 통제항목 등록 시 필요 SW 기능과 HW 속성값 선택이 요구된다. 등록된 통제항목은 모두 대안조치 관리 메뉴에서 대안조치를 등록할 수 있다. 대안조치가 등록된 통제항목은 페이지 내 통제항목 목록 우측의 수정 버튼을 통해 대안조치 내용을 수정할 수 있다.

5. 결론

오늘날 산업제어시스템은 나날이 고도화, 지능화되는 사이버 공격으로부터 그 위험성이 높아지고 있다. 이에 본 논문은 산업제어시스템의 보안상태를 점검하고 조치를 취함으로써 사이버 보안사고를 사전에 예방할 수 있도록 정보보안 관리체계 프로그램을 제안한다. 해당 프로그램은 국내 산업제어시스템 특성에 맞는 정보보안 관리체계를 제안함으로써 체계적인 보안관리를 가능케 한다. 기능적으로는 1 차적으로 사용자가 등록한 자산에 대하여 보안상태를 평가 및 조치할 수 있고 2 차적으로 중요 자산을 추적 관리할 수 있다는 장점이 있다. 또한 기존의 체크리스트 형식으로 평가하는 방법이 아닌 관리자가 직접 필요한 대안조치를 추가 등록, 관리함으로써 보안조치를 갱신할 수 있는 프로그램이기 때문에 지속적 보안 관리가 가능하다. 끝으로 빠르게 변화되고 증가하는 보안 위협에 대응할 수 있도록 능동적인 대처와 체계적인 향후 관리를 제안한다는 점에서 국내 산업제어시스템의 보안성 향상을 기대할 수 있다.

참고문헌

[1] 석병진, 김역, 이창훈, “산업제어시스템(ICS) 암호모듈 적용방안”, 2017, 한국디지털콘텐츠학회
[2] 김일용, 임희택, 지대범, 박재표, “산업제어시스템 환경에서 효과적인 네트워크 보안 관리 모델”, 2018, 한국산학기술학회 논문지
[3] 조민정, 석병진, 김역, 이창훈, “SDN 기반 산업제어시스템 제어명령 판별 메커니즘”, 2018, 한국디지털콘텐츠학회
[4] 조승한, “8 년간 한수원 해킹시도 1366 건”, 동아사이언스, 2019.10.06, http://dongascience.donga.com/news/view/31563
[5] 박향미, 유지연, “요기반시설에 대한 주요국 사이버보안 수준 비교 분석 연구”, 2017, 한국정보보호학회
[6] 이세훈, “안전한 제어시스템 구축을 위한 운영 前단계 제어시스템 보안 강화 요인에 관한 연구”, 2018, 고려대학교 정보보호대학원 사이버보안학과

본 논문은 과학기술정보통신부 정보통신창의인재양성 사업의 지원을 통해 수행한
ICT 멘토링 프로젝트 결과물입니다.